サセボ個体差調査・経過報告（横国大）

2007.8.27

（1）ＤＰＡ実験の可能性について

・第1次配布予定の30枚について，FPGA１（測定用ＦＰＧＡ）にAES-11を搭載して，AES動作時の電圧変動を測定したところ，どのボードも標準的なＤＰＡ実験で鍵推定が可能であろうことが確認できました．

（2）個体差の程度について

・ＡＥＳ動作時の電圧変動を比較すると，変動には４パターンあり，サセボには４種類あるように見えます（図１）．
・電力波形が分岐する原因を調査したところ，標準搭載されているシャント抵抗の電気的特性のばらつきに顕著な偏りがあり，これが原因だと考えられます．そう考えられる理由は，同一のシャント抵抗で測定すれば，電圧波形が同じになるからです（図2）．

・電力波形に違いがあることは，ＤＰＡ実験に影響する可能性がありますが，抵抗部品の選別が必要なほどの差異であるかどうかは，現在分析中です．

【参考】
・シャント抵抗は，利用者が差し替えて使用するものであり，違っていても問題ない，と考えれば対処は不要かもしれません．
・あるいは，シャント抵抗に差異があっても，それに影響されにくい測定法を使用すればよいかもしれません．

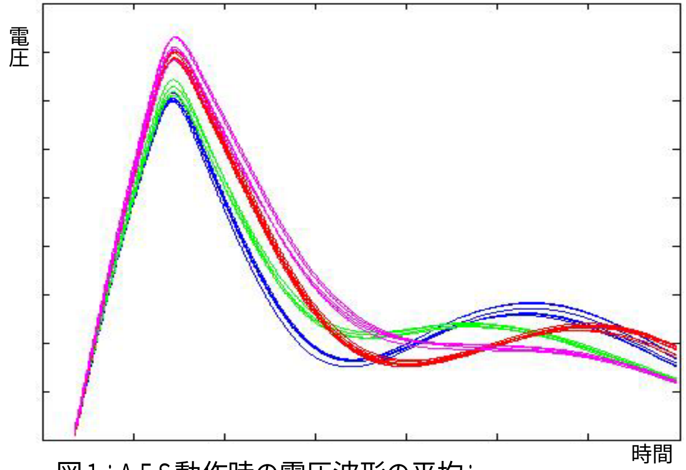


図１：ＡＥＳ動作時の電圧波形の平均：
サセボ30枚分の波形をプロット（1枚１波形）．４色に色分けしたように4グループに分かれている．

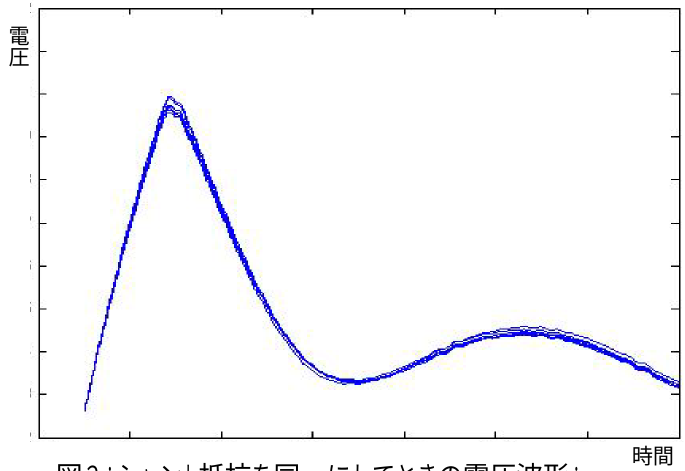


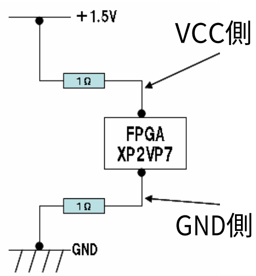
図２：シャント抵抗を同一にしてときの電圧波形：
青ボードの抵抗を他のボードに指して測定すると，青ボードの電圧波形とほぼ同じになる．

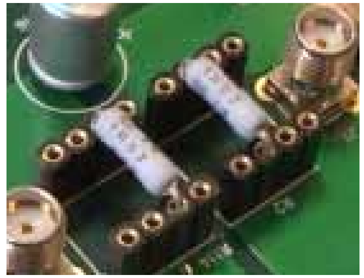
サセボ個体差調査・経過報告（横国大）

2007.8.27

【補足説明：シャント抵抗について】

・サセボの取扱説明書によると，ＦＰＧＡ１の測定用シャント抵抗は，ＶＣＣ側とＧＮＤ側の２箇所に搭載できる．





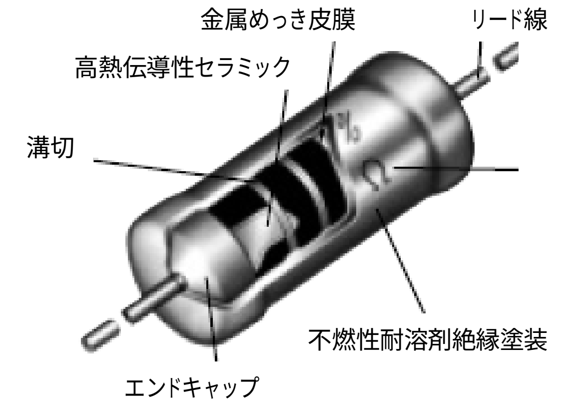
実際のシャント抵抗

・シャント抵抗は，当初は，PCN社のSMT 100m（0.1Ω，精密チップ型 シャント抵抗器）になっていたが，検討途中で 松下製 ＥＲＸ１ＳＪ（１Ω，金属皮膜抵抗，許容値±５%）に変更された．



・搭載されている抵抗値のばらつきを調べると，１Ω前後であり，許容誤差内であった（直流電流を流して電圧・電流比を測定．12本を測定して0.997Ω～1.013Ω程度）．また，サセボの４パターンとの対応も見出せなかった．

・しかし，金属皮膜抵抗は図３のようにコイル形状をしているため，誘導成分の影響が気になる．



Panasonic 金属（酸化物）皮膜固定抵抗器 カタログ，p2，構造図から

図３：金属皮膜抵抗の構成：
セラミック上に形成した金属皮膜に，らせん状に切溝を入れることで，一定長の導体にする．

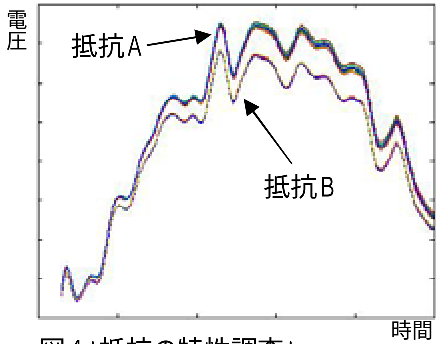


図４：抵抗の特性調査：
ＶＣＣ側，ＧＮＤ側の抵抗を合せて２２本調査．抵抗Ａは13本，抵抗Ｂは９本であった．

・そこで，インダクタンスの影響が見えるように，インパルス電流を流して電圧変動を測定すると2グループに分かれることがわかった（図４）．

・この２グループを Ａ と Ｂ とすると，
サセボの４パターンは搭載されている２本の抵抗の組合せ（Ａ－Ａ，Ａ－Ｂ，Ｂ－Ａ，Ｂ－Ｂ）と対応する．A-BとB-Aで波形が異なるのは，VCC側とGND側では，シャント抵抗以外の要素が違う（対称ではない）ためと推測される．

【対応策について】

･ボードによって（正確にはボードに搭載されているシャント抵抗によって），電力波形に多少の偏りが発生することは必ずしも致命的であるとは言えないが，標準ボードを使用する意義を考慮すると，容易に除去できる偏りは取り除いておく方が望ましいと考えられる．

0）何も知らせずに，そのまま配布する．

1）シャント抵抗がＡなのかＢなのか分るようにして，そのまま配布する．

2）１に加えて，配布する２枚のボードを組合せを，ＡＡボードとＢＢボード，あるいはＡＢボードとＢＡボードになるように調整する．

3）搭載されているシャント抵抗には少なくとも２種類があるので，組合せを ＡＢ（あるいはＢＡ）に揃える．

4）偏りの少ない抵抗を入手して配布する．あるいは差し替える．酸化金属皮膜抵抗は，100本購入しても600円程度のもの（秋葉原で）．